



**Software Engineering Institute** | Carnegie Mellon

# **Software Assurance in CMMI® Version 1.3**

Mike Konrad

September 14, 2011  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

© 2010 Carnegie Mellon University

Except for the U.S. government purposes described below, this material SHALL NOT be re-distributed, reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

# Purpose

The purpose of this presentation is to briefly describe where software assurance is addressed in the CMMI Version 1.3 models.

# Why, Historically, Software Assurance Has Been More Implicit than Explicit in CMMI<sub>1</sub>

CMMI includes practices intended to help organizations improve their capability to acquire, develop, and deliver products and services, covering such areas as:

- Process management
- Project and work group management
- Acquisition engineering
- Product (and Service System) engineering
- Service establishment and delivery
- Support (measurement and analysis, decision making, etc.)

CMMI was never intended to be specific with respect to particular:

- Industries or products
- Organizational missions or business needs or objectives
- Organizational types (e.g., for-profit, government, partnership)
- Organizational structures and environments (e.g., Line, IPPD, etc.)

# Why, Historically, Software Assurance Has Been More Implicit than Explicit in CMMI<sub>2</sub>

Thus, the practices of CMMI were written for general applicability and for a broad range of acquiring, developing/testing, service delivery missions and environments.

Each organization must interpret CMMI for its particular needs.

- Organizations that understand their *needs* and *drive* their improvements accordingly are more likely to obtain significant improvements in *performance*.
- Attributes, such as safety and security, critical to team, project, work group, or organizational performance and success, should be thought of as “*drivers*” to how CMMI practices are approached.

# Excerpts from CMMI Version 1.3 Upgrade Training

In the eight slides that follow immediately (slides 7-14), we provide excerpts from our CMMI Version 1.3 Upgrade Training to show in what ways software assurance is an explicit or implicit driver.

Then in the next nine slides (slides 15-23), we focus on particular process areas or practices to show further how software assurance-related concerns are made explicit in the informative material.

In the final slide, I reflect on the adequacy of this approach to covering software assurance in CMMI.

# (CMMI Version 1.3 Upgrade Training) Lifecycle Needs and Standards<sub>1</sub>

V1.2 models focused on the development lifecycle, but did not mention other lifecycles relevant to CMMI, including manufacturing, deployment, operations, maintenance, support, and disposal.

Thus, for V1.3:

- CMMI-DEV Part 1 references the CMMI-SVC model for lifecycles such as manufacturing and maintenance.
- In OPF SP 1.1, added an example box that provides examples of standards that could be used to reflect the organization's process needs and objectives, including lifecycle-related standards.
- Added standards entries to the References in the Appendix.

# (CMMI Version 1.3 Upgrade Training)

## Lifecycle Needs and Standards<sub>2</sub>

Added a new example box to OPF SP 1.1, subpractice 1 *[all models]*

Examples of standards include the following:

- ISO/IEC 12207:2008 Systems and Software Engineering – Software Life Cycle Processes [ISO 2008a]
- ISO/IEC 15288:2008 Systems and Software Engineering – System Life Cycle Processes [ISO 2008b]
- ISO/IEC 27001:2005 Information technology – Security techniques – Information Security Management Systems – Requirements [ISO/IEC 2005]
- ISO/IEC 14764 Software Engineering – Software Life Cycle Processes – Maintenance [ISO 2006b]
- ISO/IEC 20000 Information Technology – Service Management [ISO 2005b]
- Assurance Focus for CMMI [DHS 2009]
- NDIA Engineering for System Assurance Guidebook [NDIA 2008]
- Resiliency Management Model [SEI 2010c]

# (CMMI Version 1.3 Upgrade Training) Lifecycle Needs and Standards<sub>3</sub>

## Added References *[all models]*

### ISO/IEC 2005

International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27001 Information Technology – Security Techniques – Information Security Management Systems – Requirements*, 2005.

[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103)

### DHS 2009

Department of Homeland Security. *Assurance Focus for CMMI (Summary of Assurance for CMMI Efforts)*, 2009.

[https://buildsecurityin.us-cert.gov/swa/proself\\_assm.html](https://buildsecurityin.us-cert.gov/swa/proself_assm.html).

### NDIA 2008

NDIA System Assurance Committee. *Engineering for System Assurance*. Arlington, VA: NDIA, 2008.

<http://www.ndia.org/Divisions/Divisions/SystemsEngineering/Documents/Studies/SA-Guidebook-v1-Oct2008-REV.pdf>.

# (CMMI Version 1.3 Upgrade Training) Modernizing Development Practices<sub>1</sub>

## The Problem

Much of the engineering content of DEV V1.2 is ten years old.

As DEV was a starting point for the other two constellations, no V1.2 model adequately addresses “modern” engineering approaches now in more widespread use.

For example, RD SG 3 and RD SP 3.2 both emphasize functionality and not non-functional requirements (SSD SP 1.3 also does too).

Also, Engineering and other PAs rarely mention the following concepts:

- Quality attributes (i.e., non functional requirements or “ilities”)
- Allocation of product capabilities to release increments
- Product lines
- System of systems
- Architecture-centric development practices
- Technology maturation

# **(CMMI Version 1.3 Upgrade Training) Modernizing Development Practices<sub>2</sub>**

## **Overview of Solution**

Updated the glossary to include new terms (and modified some old terms), including quality attribute, architecture, definition of required functionality and quality attributes.

Updated the informative material in all three models (especially RD, REQM, VAL, VER) to bring more balance to functional and quality attribute requirements (non-functional requirements).

Made minimal updates to required and expected content (RD SG 3, RD SP 3.2, and SSD).

Updated the informative material in all three models to address other modern engineering approaches (e.g., product lines).

Replaced selected uses of the overloaded term “performance” in all three models with another appropriate qualifying phrase.

# (CMMI Version 1.3 Upgrade Training) Modernizing Development Practices<sub>3</sub> *[All Models]*

## Example – New terms reflecting modern engineering

### **quality attribute**

A property of a product or service by which its quality will be judged by relevant stakeholders. Quality attributes are characterizable by some appropriate measure.

Quality attributes are non-functional, such as timeliness, throughput, responsiveness, security, modifiability, reliability, and usability. They have a significant influence on the architecture.

# (CMMI Version 1.3 Upgrade Training) Modernizing Development Practices<sub>5</sub> *[All Models]*

## Example – New terms reflecting modern engineering

### **architecture**

The set of structures needed to reason about a product. These structures are comprised of elements, relations among them, and properties of both.

In a service context, the architecture is often applied to the service system.

Note that functionality is only one aspect of the product. Quality attributes, such as responsiveness, reliability, and security, are also important to reason about.

Structures provide the means for highlighting different portions of the architecture. (See also “functional architecture.”)

# (CMMI Version 1.3 Upgrade Training) Modernizing Development Practices<sub>7</sub> *[DEV only]*

Example – Minimal updates to required and expected material; and also updates to informative material

## (RD) SG 3 Analyze and Validate Requirements

*The requirements are analyzed and validated, ~~and a definition of required functionality is developed.~~*

...

A scenario is typically a sequence of events that ~~might~~*may* occur in the development, use, or sustainment of the product, which is used to make explicit some of the functional or quality attribute needs of the stakeholders.

*[From first note under SP 3.1 statement]*

...

## SP 3.2 Establish a Definition of Required Functionality and Quality Attributes

...

### Subpractices

1. Determine key mission and business drivers.

# Selected Excerpts: Work Env'mt-Related Practices in OPD & IPM *[All Models]*

## OPD SP 1.6 Establish Work Environment Standards

***Establish and maintain work environment standards.***

Work environment standards allow the organization and projects/work groups to benefit from common tools, training, and maintenance ... Work environment standards address the needs of all stakeholders and consider productivity, cost, availability, security, and workplace health, safety, and ergonomic factors...

Examples of work environment standards include the following:

- Procedures for the operation, safety, and security of the work environment ...

## IPM SP 1.3 Establish the Project's Work Environment

***Establish and maintain the project's work environment based on the organization's work environment standards.***

### Subpractices

1. Plan, design, and install a work environment for the project.

The critical aspects of the project work environment are, like any other product, requirements driven. Functionality and quality attributes of the work environment are explored with the same rigor as is done for any other product development project.

It may be necessary to make tradeoffs among quality attributes, costs, and risks...

- Quality attribute considerations can include timely communication, safety, security, ...

# Selected Excerpts: Planning Practices in PP/WP [All Models]

## SP 1.5 Estimate Effort and Cost

*Estimate **the project's** effort and cost for work products and tasks based on estimation rationale.*

3. Estimate effort and cost using models, historical data, or a combination of both. Examples of effort and cost inputs used for estimating typically include the following: ...

- Level of security required for tasks, work products, hardware, software, staff, and work environment

## SP 2.3 Plan Data Management

*Plan for the management of **project** data.*

### Example Work Products

6. Security requirements
7. Security procedures

### Subpractices

1. Establish requirements and procedures to ensure **privacy and the security** of data.

# Selected Excerpts: Risk Practices in **RSKM [All Models]**

## SP 1.1 Determine Risk Sources and Categories

***Determine risk sources and categories.***

1. Determine risk sources.

Typical internal and external risk sources include the following: ...

- Regulatory constraints (e.g. security, safety, environment)

2. Determine risk categories.

The following factors can be considered when determining risk categories:

- Product safety, security, and reliability

## SP 2.1 Identify Risks

***Identify and document risks.***

1. Identify the risks associated with cost, schedule, and performance.

Performance risks can include risks associated with the following: ...

... characteristics that enable an in-use product or service to provide required performance, such as maintaining safety and security performance

## Selected Excerpts: Other PAs *[All Models]*

CM: performing reviews to ensure that changes “have **not compromised the safety or security** of the system” *[SP 2.2 SubP 4 and a note]*

MA: examples of derived measures given include “**Information system/security** measures (e.g., percentage of **system vulnerabilities** mitigated)” *[SP 1.2 notes]*

OT: training performed by project/work group or support group includes “training in **safety, security, ...**” *[SP 1.2 SubP 2 note]*

# Selected Excerpts from CMMI-ACQ

**ARD:** “Design considerations and constraints address the **quality attributes and technical performance** that are critical to the success of the **product** in its **intended operational environment**. They account for customer requirements relative to product interoperability, implications from the use of commercial off-the-shelf (COTS) products, **safety, security, durability, and other mission critical concerns**. *[SP 2.1 Establish Contractual Requirements, Subp 3 Note]*

**PP:** “Other examples of business considerations for an acquisition strategy include the following:

- **Security issues (physical and information technology)**  
*[SP 1.1 Establish the Acquisition Strategy, Subp 3 Note]*

**SSAD:** “Examples of typical due diligence activities include the following:

- Reviews of **regulatory and security requirements**  
*[SP 2.1 Evaluate Proposed Solutions, Subp 6 Note]*

**RSKM:** “The acquirer considers risks associated with a supplier’s capability ..., including ... **security vulnerabilities** introduced by using a **supplier**.” *[SP 2.1 note]*

# Selected Excerpts from CMMI-DEV

Security and other software assurance-related concerns (particularly as example quality attributes or example stakeholder expectations) are addressed in a number of places in the Engineering process areas as implied earlier in this presentation.

There are also some CMMI-DEV-specific mentions in the core PAs, e.g.:

**PP:** “The technical approach defines a top-level strategy for development of the product. It includes decisions on ... the functionality and **quality attributes** expected in the final products, such as **safety, security**, and ergonomics.” *[SP 1.2 Establish Estimates of Work Products and Task Attributes, SubP1 note]*

# Selected Excerpts from CMMI-SVC<sub>1</sub>

IRP: “IT related security incident categories could include the following:

- Probes or scans of internal or external systems (e.g., networks, web applications, mail servers)
- Administrative or privileged (i.e., root) access to accounts, applications, servers networks, etc.
- Distributed denial of service attacks, web defacements, malicious code (e.g., viruses)
- Insider attacks or other misuse of resources (e.g., password sharing)
- Loss of personally identifiable information”

*[SP 1.1 Establish an Approach to Incident Resolution and Prevention, Subp 2 Note]*

SD: “4. Manage and control the **security** of service delivery.” and “5. Manage and control **other operationally oriented quality attributes** ...” *[SP 3.2 Operate the Service System, SubPs 4 and 5]*

# Selected Excerpts from CMMI-SVC<sub>2</sub>

**SST**: “Preparing for service system transition also requires an evaluation of the potential **impact of the transition on quality attributes**. Quality attributes are key properties of the service and service system (e.g., responsiveness, **availability, security**) **important to achieving business or mission objectives**. ...” *[SG 1 Prepare for Service System Transition, Note]*

**WP**: “8. Identify the approach used to maintain **safety and security** in the service. Attention to safety and security should be present in all major planning activities (e.g., those planning activities related to service objectives, resources, risks, stakeholders) but this subpractice suggests taking a **holistic view and focus on safety and security issues and risks, and the activities the service might include to address them**.” *[SP 1.1 Establish the Service Strategy, Subp 8 and note]*

# Selected Excerpts from CMMI-SVC<sub>3</sub>

And, assurance is a major focus of the whole Service Continuity process area:

“The purpose of Service Continuity (SCON) is to establish and maintain plans to ensure continuity of services during and following any significant disruption of normal operations.”

## “Specific Goal and Practice Summary

SG 1 Identify Essential Service Dependencies

SP 1.1 Identify and Prioritize Essential Functions

SP 1.2 Identify and Prioritize Essential Resources

SG 2 Prepare for Service Continuity

SP 2.1 Establish Service Continuity Plans

SP 2.2 Establish Service Continuity Training

SP 2.3 Provide and Evaluate Service Continuity Training

SG 3 Verify and Validate the Service Continuity Plan

SP 3.1 Prepare for the Verification and Validation of the Service Continuity Plan

SP 3.2 Verify and Validate the Service Continuity Plan

SP 3.3 Analyze Results of Verification and Validation of the Service Continuity Plan”

# Mike's Perspective on This

We've seen that CMMI Version 1.3 includes a lot of material that encourages addressing software assurance (e.g., safety and security).

- Almost all of it is in the informative material.

While there may have been reasons for taking a more conservative approach to covering software assurance in the past, its very nature requires increasing attention, coordination, and learning.

- A role for CMMI is to identify which knowledge areas are critical to business success and are worthy of more explicit attention.

Without making explicit the need for software assurance in CMMI required and expected material are we (those who help sustain the model) communicating to organizations that they need not explicitly address software assurance in a strategic and holistic way?

- In the past few years, we've seen more organizations ask for extensions to CMMI to address software assurance-related topics